УДК 316.774:004.738

И. Л. Лукашкова
доцент кафедры социально-гуманитарных дисциплин
Могилевского института МВД,
кандидат педагогических наук (Беларусь)

ИНФОРМАЦИОННО-КОММУНИКАТИВНЫЕ УГРОЗЫ ВИРТУАЛЬНОГО ВЗАИМОДЕЙСТВИЯ: ОСОБЕННОСТИ ПРОЯВЛЕНИЯ И СПОСОБЫ РЕАЛИЗАЦИИ

В статье рассматриваются угрозы виртуальной среды в контексте коммуникаций и особенности их проявления. Раскрыты формы проявления агрессивного поведения в Интернете и их негативные последствия для пользователей. Автором обозначены и охарактеризованы негативные явления сетевого пространства: кибербуллинг и его формы (секстинг, флейминг, харассмент, троллинг, киберсталкинг), социальная инженерия, вербовочная и пропагандистская деятельность экстремистских и религиозных организаций, действия мошеннических атак и лиц с психическими отклонениями.

INFORMATION AND COMMUNICATIVE THREATS OF VIRTUAL INTERACTION: FEATURES OF MANIFESTATION AND WAYS OF REALIZATION

Formation of the World wide web and its further development promoted creation of the new communicative platform. It not only gave to users other opportunities and advantages, but also initiated the communicative resources and specifics of functioning a set of risks.

The relevance of a problem of definition and detailed studying of information and communicative threats of network communications is caused by globality of their negative consequences for health and safety of users of Network. Researchers refer speech aggression, cyberbullying and its forms (a seksting, a fleyming, harassment, trolling, a kiberstalking), social engineering, recruiting activity of the extremist and religious organizations, actions of the fraudulent attacks and mentally-disordered persons to the most widespread information and communicative threats of virtual space. The information and communicative threats characterized in article do not exclude a possibility of emergence of other risks with development of Internet technologies. The complex research of new forms of information and communicative threats should be considered as a necessary condition and the scientific basis for search and development of effective ways and warning facilities and protection of participants of the virtual environment.

Интенсивное развитие и внедрение компьютерных технологий практически во все сферы жизнедеятельности современного человека, формирование Всемирной сети и активное использование ее ресурсов привело к возникновению совершенно иной (по возможностям и воздействию) коммуникативной

платформы. Особенности этого глобально-виртуального пространства коммуникации в последние годы являются объектом пристального внимания представителей научных сообществ различных областей знания. Наибольшую актуальность вызывают вопросы, связанные с исследованием угроз сетевых коммуникаций.

М. Кастельс, автор теории «сетевого общества», развивший ее в рамках логики концепции постиндустриального общества, полагает, что для нового типа общества характерна трансформация многих видов деятельности человека согласно сетевой логике [1].

Наблюдаются значительные изменения в журналистской и литературной деятельности. Формирование новостной повестки, сбор, анализ и распространение информации уже перестали быть прерогативой профессиональных журналистов. Развитие Интернета и цифровых технологий способствовало появлению и масштабному распространению гражданской журналистики, когда освещением событий занимаются обычные граждане. В настоящее время в создании контента для новых медиа зачастую принимают участие даже не сотни, а тысячи людей, проживающих в разных странах. Такие явления — результат функционирования нового сетевого пространства коммуникации, которое характеризуется децентрализованностью, открытостью, гибкостью и горизонтальной направленностью перемещения коммуникативного потока.

Подобная тенденция присуща и взаимодействию в виртуальной среде на межличностном уровне. Высокую привлекательность интернет-пространства как коммуникативной платформы обусловливают ее демократичность, глобальность и интерактивность. Кроме того, функциональность инструментов, обеспечивающих поиск, связь, передачу информации не только удовлетворяет самые разнообразные потребности пользователей, но и минимизирует временные, физические и материальные затраты.

В качестве еще одного преимущества интернет-коммуникации следует выделить достаточно простую процедуру авторизации и модерации. В ряде случаев она предусматривает лишь введение логина, пароля и адреса электронной почты для того, чтобы стать участником виртуального взаимодействия. При этом пользователь для опосредованной самопрезентации может использовать как персональные данные, так и вымышленные, не соответствующие его реальной личности. Низкая степень ограничений предоставляет широкие возможности для самопрезентационного поведения, «многоликости», идентификации себя с желаемой возрастной, половой, этнической, социальной, профессиональной группой, что способствует размыванию границ и форм коммуникатив-

ного поведения, установлению равноправных отношений между коммуникантами.

Однако перечисленные достоинства не исключают наличия ряда угроз безопасности пользователей сетевой коммуникации, связанных с отсутствием запретов на фальсификацию информации в процессе самопрезентации, открытостью и доступностью коммуникативных платформ в Интернете.

Высокий уровень опасности и распространенности в сетевом пространстве представляют коммуникативные риски, к которым можно отнести демонстрацию речевой агрессии виртуальными собеседниками. По мнению Е. Н. Басовской, речевая агрессия — вид доминирующего речевого поведения, которое вербально может проявляться в грубости, оскорблении, хамстве, сарказме, нецензурных выражениях [2]. Но Т. И. Стексова полагает, что речевая агрессия в виртуальных коммуникациях обусловлена общим эмоциональным фоном и негативным отношением к социуму [3]. Тем не менее даже при отсутствии у пользователя преднамеренного желания оскорбить или унизить участников виртуальной беседы речевая агрессия несет угрозу как для партнеров коммуникации, так и для пассивного читателя. Отзывы отрицательного характера, размещаемые на форумах и новостных площадках, вызывают негативные эмоциональные переживания и деструкцию коммуникативных стратегий, а в некоторых случаях уязвленный человек может стать потенциальным агрессором.

К более серьезным информационно-коммуникативным угрозам следует отнести кибербуллинг. Высокая социальная опасность данного явления связана с вовлечением в него детей и подростков. По определению А. А. Бочавер и К. Д. Хломова, кибербуллинг — новая и активно распространяющаяся во всем мире форма травли посредством использования возможностей Интернета. Для реализации своих действий кибербуллеры могут применять практически все коммуникативные ресурсы виртуальной среды: электронную почту, мгновенные сообщения, веб-страницы, блоги, форумы и чаты, MMS- и SMS-сообщения, онлайн-игры. Авторы указывают, что кибербуллинг может быть прямым, когда агрессор непосредственно атакует жертву, посылая ей письма или сообщения грубого, оскорбительного характера. Косвенный кибербуллинг предполагает вовлечение в процесс травли определенного круга лиц. Преследователь осуществляет взлом аккаунта жертвы или создает его «фейковую» копию, а затем рассылает с него компрометирующие сообщения людям, составляющим круг виртуальных (часто реальных) знакомых жертвы. Тем самым агрессор дискредитирует личность жертвы и оказывает разрушающее воздействие на ее коммуникативное поле [4].

Также А. А. Бочавер и К. Д. Хломов выделяют различные формы кибербуллинга:

- секстинг — это рассылка материалов сексуального характера, вызывающих у жертвы спектр негативных эмоциональных реакций;

- флейминг — эмоционально бурный процесс быстрого обмена репликами, содержащими оскорбления;

- харассмент — настойчивое и длительное отправление жертве повторяющихся оскорбительных сообщений, направленное на ее моральное уничтожение;

- троллинг (одна из форм харассмента) — публикация на веб-сайтах, страницах социальных сетей негативной информации, провокационных сообщений с целью подведения человека к агрессивной реакции и развития конфликта;

- кибersталкинг — преследование человека в виртуальном пространстве посредством атаки манипулятивными сообщениями, угроз противозаконных действий и повреждений, вызывающих у жертвы страх, стыд, тревогу [4].

Кибербуллинг имеет высокие информационно-коммуникативные риски, которые могут вызвать дестабилизацию эмоциональной сферы пользователя, расстройства личности, деформацию коммуникативных стратегий, дезориентацию, а в крайних случаях — депрессивные расстройства и суицид.

Среди действующих угроз безопасности пользователей следует выделить социальную инженерию, вербовочную деятельность экстремистских и религиозных организаций, действия мошеннических атак и лиц с психическими отклонениями, которые также проявляют свою активность в сетевом пространстве. Они отличаются от рассмотренных выше рисков интернет-коммуникаций сложностью выявления, неясностью целей и мотивов атакующих лиц.

В работе М. В. Кузнецова и И. В. Симдянова социальная инженерия определяется как манипуляция одним или несколькими людьми, целью которой является взлом систем безопасности и похищение важной информации [5]. Особенностью социальной инженерии является то, что хакерской атаке подвергается не компьютер, а человек, работающий за компьютером. Основными способами воздействия социальных хакеров, с помощью которых они получают конфиденциальную информацию, выступают обман, запугивание, шантаж, угрозы, провокации, обещания, подкуп, предложения. Эти методы приводят к дезориентации и деструктивной активности человека, отвечающего за безопасность секретной информации. Деятельность социальных хакеров наносит серьезный вред психологическому здоровью объектов воздействия и создает значительные угрозы информационной безопасности пользователей.

Существенную опасность для участников сетевых коммуникаций представляют экстремисты и представители различных религиозных организаций. Т. В. Жаворонкова отмечает, что, пропагандируя свои цели и идеи, осуществляя поиск сподвижников и вербовку сторонников, экстремисты активно используют интернет-ресурсы для публикации статей и призывов радикального толка на страницах форумов, социальных сетей, размещения фото- и видеоконтента с ложными идеями и убеждениями [6]. Кроме того, экстремисты на основании тщательного анализа личностных особенностей пользователей проводят отбор кандидатур, наиболее уязвимых для их пропаганды. Выявление экстремистской деятельности — достаточно сложная задача, поскольку инструментальный набор социальных сетей предоставляет возможность фальсификации личности, создания образа, располагающего к доверительным отношениям. Следствия информационного воздействия экстремистов могут заключаться в психоэмоциональных нарушениях, склонностях к делинквентному поведению, деформации социально-нравственных ориентиров.

Подобные неблагоприятные последствия посетители интернет-пространства испытывают и в результате манипулятивных действий представителей неофициальных религиозных сообществ (сект). Следовательно, информационную опасность представляют как радикально настроенные организации, так и деструктивные религиозные сообщества.

Еще одна группа посетителей виртуальной среды, представляющая угрозу для современных пользователей, — это лица с психическими патологиями. Так, исследованиями В. Д. Менделевича выявлено, что пользователи с шизофренией, шизотипическим расстройством, личностным, невротическим и соматоформным расстройствами имеют повышенный интерес к сетевым коммуникациям. Взаимодействие с такими участниками безопасно, если их психическое заболевание находится в невыраженной форме, а поведение контролируется. В противном случае посетители коммуникативной платформы могут стать объектами агрессивных реакций, манипуляций, проявлений патологической зависимости.

Не менее серьезную угрозу для пользователей виртуального коммуникативного пространства представляет группа лиц с сексуальными девиациями. Интернет-платформу они рассматривают как возможность удовлетворения своих патологических потребностей. С этой целью они устанавливают доверительные отношения со своей жертвой, а затем вовлекают ее в интимную переписку, видеосвязь. Часто жертва, испытавшая информационное насилие такого рода, переживает страх, смятение, стыд, тревогу. Подобные явления представляют значительную информационно-коммуникативную опасность не только

для детской аудитории, но и для взрослых, поскольку объектом домогательств может стать любой открытый для диалога пользователь.

Таким образом, формирование Всемирной паутины и ее дальнейшее развитие способствовало созданию новой коммуникативной платформы. Она не только предоставила пользователям иные возможности и преимущества, но и инициировала своими коммуникативными ресурсами и спецификой функционирования множество рисков.

Актуальность проблемы определения и детального изучения информационно-коммуникативных угроз сетевых коммуникаций обусловлена глобальностью их негативных последствий для здоровья и безопасности пользователей Сети.

К наиболее распространенным информационно-коммуникативным угрозам виртуального пространства исследователи относят речевую агрессию, кибербуллинг и его формы (секстинг, флейминг, харассмент, троллинг, кибер-сталкинг), социальную инженерию, вербовочную деятельность экстремистских и религиозных организаций, действия мошеннических атак и лиц с психическими отклонениями. Охарактеризованные в статье информационные и коммуникативные угрозы не исключают возможности появления иных рисков с развитием интернет-технологий. Комплексное исследование новых форм информационно-коммуникативных угроз следует рассматривать как необходимое условие и научное основание для поиска и разработки эффективных способов и средств предупреждения и защиты участников виртуальной среды.

Список основных источников

1. Кастельс, М. Галактика Интернет: Размышления об Интернете, бизнесе и обществе / М. Кастельс. — Екатеринбург : У-Фактория, 2004. — 328 с. Вернуться к статье

2. Басовская, Е. Н. Творцы черно-белой реальности: о вербальной агрессии в средствах массовой информации / Е. Н. Басовская // Критика и семиотика. — 2004. — Вып. 7. — 2004. — С. 257–263. Вернуться к статье

3. Стексова, Т. И. Речевая агрессия в интернет-комментариях как проявление социальной напряженности / Т. И. Стексова // Политическая лингвистика. — 2013. — № 3. — С. 77–81. Вернуться к статье

4. Бочавер, А. А. Кибербуллинг: травля в пространстве современных технологий / А. А. Бочавер, К. Д. Хломов // Психология. Журнал высшей школы экономики. — 2014. — № 3. — С. 177–191. Вернуться к статье

5. Кузнецов, М. В. Социальная инженерия и социальные хакеры / М. В. Кузнецов, И. В. Симдянов. — СПб : БХВ-Петербург, 2007. — 368 с. Вернуться к статье

6. Жаворонкова, Т. В. Использование сети Интернет террористическими и экстремистскими организациями / Т. В. Жаворонкова // Вестн. Оренбургского гос. ун-та. — 2015. — № 3. — С. 30–37. Вернуться к статье